IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-1315
	)	
v.	)	
	)	
ANDREY GHINKUL	)	
a/k/a Andrei Ghincul	)	
a/k/a "smilex,"	)	
	)	
MAKSIM VIKTOROVICH YAKUBETS	)	
a/k/a "aqua,"	)	
	)	
IGOR TURASHEV	)	
a/k/a "nintutu,"	)	
	)	
MAKSIM MAZILOV	)	
a/k/a "caramba," and,	)	
	)	
ANDREY SHKOLOVOY	)	
a/k/a "caramba,"	)	
	)	
Defendants.	)	

AMENDED PRELIMINARY INJUNCTION

Plaintiff, the United States of America, filed a complaint for injunctive relief pursuant to 18 U.S.C. §§ 1345 and 2521, based on the defendants' violations of 18 U.S.C. §§ 1343, 1344, and 2511, and moved for a temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure and 18 U.S.C. §§ 1345(a)(1) and 2521. On October 9, 2015, this Court granted the Government's application for a temporary restraining order and order to show cause why a preliminary injunction should not be granted against Defendants Andrey Ghinkul, Maksim Viktorovich Yakubets, Igor Turashev, Maksim Mazilov, and Andrey Shkolovoy. On October 19, 2015, this Court granted the Government's Motion for Preliminary Injunction.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

The Court has considered the Government's Motion to Modify the Preliminary Injunction, and hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against the defendants under 18 U.S.C. §§ 1345 and 2511.

2. There is good cause to believe that the defendants have engaged in and are likely to engage in acts or practices that violate 18 U.S.C. §§ 1343, 1344, and 2511, and that the Government is, therefore, likely to prevail on the merits of this action.

3. There is good cause to believe that, unless the defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the defendants' ongoing violations of 18 U.S.C. §§ 1343, 1344, and 2511. The evidence set forth in the Government's Memorandum of Law, and the accompanying declaration, demonstrate that the Government is likely to prevail on its claim that the defendants have engaged in violations of 18 U.S.C. §§ 1343, 1344, and 2511 by:

a. intentionally infecting hundreds of thousands of computers with malicious software ("malware") to steal banking and other online credentials from infected computers and enlist those computers into the Bugat/Dridex "botnet" (network of infected computers controlled by the defendants);

b. using the Bugat/Dridex malware to intercept victims' communications without authorization;

c. using credentials stolen by the Bugat/Dridex malware to access victim bank accounts and fraudulently transfer funds; and

d. intentionally infecting thousands of computers worldwide with the malware Bugat/Dridex.

4. There is good cause to believe that if such conduct continues, it will cause irreparable harm to both individuals and businesses in the United States. There is also good cause to believe that the defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. Based on the evidence cited in the Government's Memorandum of Law (Doc. 11) and accompanying declaration (Doc. 12) and exhibits, the Government is likely to be able to prove that the defendants are engaged in activities that violate United States law and harm members of the public, and that the defendants have continued their unlawful conduct despite the clear injury to members of the public.

6. The Government has demonstrated good cause to believe that the defendants have directed their illegal activity at individuals and businesses located in the Western District of Pennsylvania by, among other things, infecting numerous computers in this District with Bugat/Dridex and by using credentials stolen by the Bugat/Dridex malware to gain unauthorized access to the bank accounts of victims in this District.

7. The Government has demonstrated good cause to believe that to immediately halt the injury caused by the defendants, the defendants must be prohibited from infecting computers with Bugat/Dridex and from communicating with existing computers infected with Bugat/Dridex malware.

8. Based on the Government's Memorandum of Law in Support of Motion to Modify the Preliminary Injunction, there is good cause to believe that it is no longer necessary to require that the companies and organizations identified in Appendix A redirect inbound traffic to identified super-peers to computer(s) controlled by the United States.

AMENDED PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED that the defendants, their representatives, and persons who are in active concert or participation with them are restrained and enjoined from using malicious software or code in furtherance of any scheme to commit wire fraud, bank fraud, or to engage in unauthorized interception of electronic communications, and in particular, are prohibited from running, controlling, or communicating with software known as Dridex (the most recent iteration of the Bugat/Dridex family of malware), on any computers not owned by the defendants.

IT IS FURTHER ORDERED that the Government is authorized to continue to operate substitute server(s) and other computer infrastructure as specified in the Government's Memorandum of Law (Doc. 11) that, in conjunction with the relief ordered below, replaces the defendants' command and control infrastructure for the Bugat/Dridex botnet and identified super peers and severs the defendants' connection to the infected computers in the Bugat/Dridex botnet. Pursuant to the Pen Register Trap and Trace Order signed on October 9, 2015, and renewed on December 8, 2015, the Government is authorized to collect dialing, routing, addressing and signaling ("DRAS") information from the infected computers that connect to the infrastructure created pursuant to this Order. The Government shall ensure that no electronic

content or other non-DRAS information is collected when victim computers connect to the infrastructure established pursuant to this Order.

IT IS FURTHER ORDERED that copies of this Order shall be served as follows:

1. Via a Mutual Legal Assistance Treaty request for delivery upon defendant Ghinkul at his custodial location in Cyprus;

2. Via electronic messages to Mazilov and Shkolovoy sharing "caramba," Yakubets as "aqua," and Turashev as "nintutu" at their last known email addresses; and

4. Via publication on the Internet websites of the Department of Justice (http://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled) and the Federal Bureau of Investigation (linked to the Department of Justice website).

Entered this 22nd day of December, 2015 at 10:30 a.m.

s/ Terrence F. McVerry
HON. TERRENCE F. McVERRY
UNITED STATES DISTRICT JUDGE